AMENDMENTS TO THE CLAIMS

Claims 1 – 28 (canceled).

29. (Currently amended) A method for assisting a user in verifying a cast ballot B_{cast} stored in a server, the method comprising:

forming a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$;

associating the B_{cast} and $DS(B_{cast}, s)$ with a vote serial number VSN;

forming a confirmation token, comprising $DS(B_{cast}, s)$ and VSN;

making the confirmation token available to a user;

receiving a confirmation token made available to a user;

extracting $VSN_{received\ token}$ and $DS_{received\ token}(B_{cast}, s)$ from the received token; and

for VSN equal to $VSN_{received\ token}$, comparing $DS_{received\ token}(B_{cast}, s)$ and at least one of $DS(B_{cast}, s)$ and $DS(B_{cast}, S)$;

if the comparison shows equivalence between the data compared, determining that B_{cast} is verified.

30. (Previously Presented) The method of Claim 29 wherein:

the confirmation token further comprises a digital signature of an aggregation comprising the associated B_{cast} and VSN using the server's private key DS(Aggregation, s),

extracting $DS_{received\ token}$ (Aggregation, s) from the received token; and

B_{cast} is verified only upon the additional condition that $DS_{received\ token}$ (Aggregation, s) is equivalent to DS(Aggregation, s).

31. (Currently amended) A method for assisting a user in verifying a cast ballot recorded in a server, the method comprising:

receiving in a server at least one set of:

a cast ballot B_{cast} and

a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$;

forming:

a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$,

associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN;

forming a confirmation token, comprising:

$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s),

where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN;

making the confirmation token available to a user;

receiving a confirmation token

extracting $VSN_{received\ token}$ and at least one of $DS_{received\ token}(B_{cast}, s)$, $DS_{received\ token}(B_{cast}, v)$, and $DS_{received\ token}(AG, s)$ from the received token; and

for $VSN_{received\ token}$ and the corresponding VSN, comparing at least one of:

$DS_{received\ token}(B_{cast}, s)$ and $DS(B_{cast}, S)$;

$DS_{received\ token}(B_{cast}, v)$, and $DS(B_{cast}, v)$;

$DS_{received\ token}$(Aggregation, s), and DS(Aggregation, s);

if comparison shows equivalence between the data compared, determining that B_{cast} is verified.

32. (Previously Presented) The method of Claim 31 further comprising:

if comparison shows equivalence between $DS_{received\ token}$(Aggregation, s), and DS(Aggregation, s), determining that the received confirmation token has not been modified since its formation.

33. (Currently Amended) A method for assisting a user verifying a cast ballot recorded in a server, the method comprising:

receiving a cast ballot ("B_{cast}") in a server;

forming a digital signature of B_{cast} using a private key of the server ("$DS(B_{cast}, s)$"),

associating B_{cast} and $DS(B_{cast}, s)$ with a vote serial number ("VSN");

for VSN, comparing $DS(B_{cast}, s)$ and $DS(B_{cast}, S)$,

if comparison shows equivalence between the data compared, determining that B_{cast} is verified.